No. 24-1773

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

REAL TIME MEDICAL SYSTEMS, INC.

Plaintiff-Appellee,

v.

POINTCLICKCARE TECHNOLOGIES, INC.,
d/b/a PointClickCare,

Defendant-Appellant.

On Appeal from the United States District Court
for the District of Maryland,
No. 8:24-cv-00313-PX, Hon. Paula Xinis

Appellant's Opening Brief

William C. Jackson
GOODWIN PROCTER LLP
1900 N Street NW
Washington, DC 20036

Nicole Bronnimann
KING & SPALDING LLP
1100 Louisiana Street
Suite 4100
Houston, TX 77002

Rod J. Rosenstein
Jeremy M. Bylund
Counsel of Record
Amy R. Upshaw
Joshua N. Mitchell
KING & SPALDING LLP
1700 Pennsylvania Avenue NW
Washington, DC 20006
(202) 737-0500
jbylund@kslaw.com

Counsel for PointClickCare Technologies Inc.

September 16, 2024

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 24-1773 Caption: Real Time Medical Systems, Inc. v. PointClickCare Technologies, Inc.

Pursuant to FRAP 26.1 and Local Rule 26.1,

PointClickCare Technologies Inc. d/b/a PointClickCare
(name of party/amicus)

who is Appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☑ YES ☐ NO
If yes, identify all parent corporations, including all generations of parent corporations:

PointClickCare Technologies Inc. ("PCC") is a wholly owned subsidiary of PointClickCare Corp.

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

No publicly-held corporation or publicly held entity owns 10% or more of (PCC's) stock.

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☑NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/ Jeremy M. Bylund Date: 9/16/2024

Counsel for: PointClickCare

Print to PDF for Filing

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Regulations

Other Authorities

INTRODUCTION

The district court committed multiple reversible errors in entering a dangerous and unprecedented preliminary injunction that bars PointClickCare, an electronic health information ("EHI") custodian, from preventing automated third-party software "bots" from accessing and harming its software-as-a-service ("SaaS") platform. The legally defective injunction must be set aside.

More than a million patients across North America rely on PointClickCare's secure and stable platform to maintain and protect their EHI. Those health records track patients' symptoms, medical conditions, medications, and other ongoing treatments. It is critical that medical personnel have prompt, stable, and secure access to obtain an accurate picture of a patient's condition. That health information is also deeply private and must be protected from unauthorized disclosure and unauthorized alteration. Improper access can yield devastating results: patients could be given improper treatments—like contraindicated medications—that could risk their health or even their lives. Congress enacted multiple laws that prescribe a careful legislative balance to accommodate the competing interests of data security and reliable EHI

access. Privacy and security are safeguarded by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), along with the criminal and civil protections of the Computer Fraud and Abuse Act. And the 21st Century Cures Act encourages interoperability and exchange of health information among authorized information custodians to ensure that the healthcare providers have access to patients' data when they need it.

Like many custodians responsible for protecting the security and integrity of sensitive data, PointClickCare has long prohibited customers from using bots to access its platform.[1] Just this year, however, Real Time Medical Systems, Inc. ("RTMS") sued PointClickCare and asked the district court to disregard that prohibition. RTMS urged the court to disrupt Congress's holistic statutory scheme of security and access and instead require that PointClickCare give RTMS's bots unfettered access to PointClickCare's platform.

---

[1] Bots are automated software programs designed to perform tasks without human intervention. Their purpose is to perform repetitive tasks much more quickly than humans can perform them. *See* AO Kaspersky Lab, *What are bots?—Definition and Explanation* (2024), https://tinyurl.com/3pz6ha45.

RTMS and PointClickCare do not have a contractual relationship. Instead, RTMS accesses PointClickCare's platform by having PointClickCare's customers create login IDs for RTMS. As a user given access to the platform by PointClickCare's customers, RTMS is bound by the same access rules as those customers, as prescribed under PointClickCare's master subscription agreements. Among the rules every customer accepts is a prohibition on bot usage. While RTMS can access all the data it requires through human users making individual requests (as PointClickCare's customers do), RTMS maintained that it has a right to disregard PointClickCare's policy and the customers' contracts by using bots to access the data.

RTMS sought an injunction based on the dubious legal theory that PointClickCare's efforts to protect its system from bots amount to prohibited "information blocking" under the Cures Act. Stymied by the fact that the Cures Act does not provide a private right of action, RTMS sought to bootstrap its Cures Act theory as a predicate for state-law claims.

The district court obliged, fundamentally misreading the Cures Act and misinterpreting state law. First, the court ignored that the default

position under the Cures Act is *standardized* access—and so when an EHI custodian cannot reach an agreement with a requestor for *nonstandard* access, it may share EHI according to federally approved standards. PointClickCare undisputedly provides RTMS with that standardized access, but the district court nevertheless concluded that PointClickCare violated federal law by not giving RTMS everything it wanted in the precise fashion it wanted to get it. Second, the court misapplied the burden of proof to two other exceptions to the Cures Act's information-blocking definition. And third, the court turned the preliminary-injunction standard on its head by accepting RTMS's perfunctory factual presentation at face value. At a brief evidentiary hearing, the court shifted to PointClickCare the burden to demonstrate that RTMS's bots were dangerous to its system. Applying a more demanding standard to PointClickCare than it applied to RTMS, the district court ruled that PointClickCare had not offered enough evidence to prove that third-party bots are a systemic security risk to its platform—an obvious point that should not require documentation. The court then entered a dangerous and legally deficient injunction.

The court-mandated rollback of PointClickCare's data-security features poses grave danger to the health and privacy of millions of patients across two countries. The routine security measures banned by the district court protected PointClickCare's EHI not just from RTMS's disruptive bots, but also from those of unknown malicious actors.

PointClickCare seeks this expedited appeal to prevent harm to patients and healthcare providers and restore PointClickCare's authority to carry out its duty to safeguard the security and integrity of their EHI.

JURISDICTIONAL STATEMENT

The United States District Court for the District of Maryland had subject-matter jurisdiction of this action under 28 U.S.C. §§ 1331 and 1367. This Court has jurisdiction over this interlocutory appeal of an order entering a preliminary injunction under 28 U.S.C. § 1292(a).

STATEMENT OF ISSUES

1. Did the district court commit an error of law by misconstruing the Cures Act?

2. Did the district court commit an error of law by misapplying Maryland law?

3. Did the district court abuse its discretion in weighing irreparable harm, balance of equities, and public policy?

BACKGROUND

Defendant PointClickCare is a leading provider of comprehensive, cloud-based SaaS solutions for the senior-care industry in North America, providing a platform for the secure storage, processing, and analysis of EHI for more than one million patients of PointClickCare's thousands of customers. The customers are skilled nursing facilities, assisted living facilities, senior living facilities, and providers of in-home care. JA235 ¶¶ 4-5.

Plaintiff RTMS purports to provide an EHI-analysis service to a fraction of PointClickCare's customers. RTMS has no agreement with PointClickCare to access PointClickCare's platform in a safe, non-disruptive, and integrated manner. Nor does RTMS pay PointClickCare for access. Instead, RTMS employs software bots using login IDs provided by PointClickCare customers, whose contracts prohibit using such software bots. The bots enable RTMS to conduct high-frequency, mass exfiltration of patient EHI—which RTMS can repackage for its commercial purposes. RTMS's bot attacks strain PointClickCare's systems, causing slowdowns and outages that put patients' lives at risk.

PointClickCare engaged in an exhausting game of Whac-A-Mole with RTMS, in which PointClickCare employed increasingly restrictive electronic measures to thwart software bots, and RTMS intentionally defeated PointClickCare's security procedures so it could maintain its unlimited, unauthorized access. JA1115, JA1303, JA1403; JA725-732, JA738-745. When PointClickCare finally found a system to block high-volume bots that RTMS could not circumvent, RTMS filed suit. It convinced the court to enter an unprecedented injunction prohibiting PointClickCare from blocking RTMS's bots. That injunction cannot be squared with the federal government's extensive statutory framework governing access to EHI and data security.

A. Legal Background

Because of the importance and sensitivity of patient EHI, federal laws govern EHI data custodians through a tapestry of interlocking obligations. These requirements balance the need to secure deeply private health information and the need to share that information with patients and healthcare providers. An extensive administrative regime undergirds Congress's statutory structure.

Federal Data-Security Requirements. EHI custodians like PointClickCare must comply with various healthcare information and privacy laws, including HIPAA, as amended by HITECH. HIPAA requires PointClickCare to "[e]nsure the confidentiality, integrity, and availability" of EHI and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306. HIPAA also requires PointClickCare to implement policies to detect, contain, and correct security violations. *Id.* § 164.308.

Because PointClickCare's systems are used in interstate commerce, obtaining information from those systems by exceeding authorized access is a federal crime. 18 U.S.C. § 1030(a)(2); *id.* § 1030(e)(2)(B). And exceeding authorized access that results in the modification or impairment (or even the potential for either) of medical examination, diagnosis, treatment, or care of any person also yields civil liability. *Id.* § 1030(g); *see id.* § 1030(c)(4)(A)(i)(II).

The Cures Act. The 21st Century Cures Act of 2016, Pub. L. No. 114-255, requires EHI custodians like PointClickCare to ensure that patients can access and share their EHI. Before the Act, each EHI custodian could employ its own proprietary data format on its own data

repository. But those siloed EHI repositories inhibited sharing important medical-history information among providers. Congress accordingly determined that EHI custodians should share a common baseline of interoperability and information exchange. The Cures Act bars "information blocking"—any practice "likely to interfere with, prevent, or materially discourage access, exchange, or use of [EHI]" so long as the custodian "knows, or should know" that the practice is likely to have that effect. 42 U.S.C. § 300jj-52(a)(1)(A) & (a)(1)(B)(i).

At the same time, Congress wanted the EHI platforms to be secure from unfettered access to sensitive private information. To ensure a well-functioning and secure EHI exchange—and to avoid placing custodians in the position of having to violate federal privacy laws in order to comply with federal information-sharing law—Congress commanded the Department of Health & Human Services ("HHS") to identify activities that "do not constitute information blocking" because they are "reasonable and necessary." 42 U.S.C. § 300jj-52(a)(3).

Implementing Regulations. HHS identified eight classes of "reasonable and necessary activities" that it codified in regulations. *Id.*; 85 Fed. Reg. 25,642, 25,649 (May 1, 2020). The regulations include

provisions that allow a custodian to decline to share information to prevent harm, maintain privacy, protect a system's security, reject infeasible requests, or maintain an IT system's performance. *See* 45 C.F.R. §§ 171.201, 171.202, 171.203, 171.204, 171.205. Other provisions govern the manner and scope of information sharing, giving custodians a series of choices for how to share EHI. 45 C.F.R. §§ 171.301, 171.302, 171.303. Custodians may, for example, license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met, and they may charge reasonable fees for using their systems to transfer EHI. 45 C.F.R. § 171.303.

Three of these necessary activities are implicated by this litigation.

First, the "manner exception," 45 C.F.R. § 171.301, allows an actor to limit the manner in which it fulfills a request to access, exchange, or use EHI. This exception gives custodians the flexibility to enter into mutually agreeable arrangements for information sharing with qualified requestors. But where a custodian "cannot reach agreeable terms with the requestor," *id.* § 171.301(a), the custodian need not accede to the requestor's particular access request but may instead provide a federally recognized data set, such as United States Core Data for Interoperability

("USCDI"), or access through a system certified to Part 170 standards, *id.* § 171.301(b); *see* 45 C.F.R. § 170.213 (USCDI standard); JA1173 (noting that USCDI version 1 is the applicable content standard under part 170 until January 1, 2026). In its rulemaking, HHS made clear that custodians are not required to redesign their systems to accommodate third parties' demands for nonstandard access or turn over their proprietary technology on whatever terms a requestor demands: "[A]ctors who cannot reach agreeable terms with the requestor to fulfill the request are *not* required to license their IP to proprietary technology …." 85 Fed. Reg. at 25,877.

Second, the "[h]ealth IT performance exception," 45 C.F.R. § 171.205, establishes that it is not information blocking for a custodian to take reasonable and necessary measures for the benefit of the overall performance of the health information technology ("IT"), even where those measures may temporarily limit the health IT's availability or degrade its performance. The exception allows for necessary system maintenance and improvements. A key provision of this exception explicitly authorizes custodians to limit "third-party application[s]"—like bots—that "negatively impact … performance." *Id.* § 171.205(b).

And, *third*, the "[s]ecurity exception," 45 C.F.R. § 171.203, allows a custodian to limit the access, exchange, or use of EHI in order to protect EHI security.

Each of these activities is reasonable and necessary for the national system of EHI exchange, so conduct falling within any of the exceptions is not information blocking.

Enforcement regime. The Cures Act provides for enforcement by the federal government with no private right of action. The office of the "inspector general of the Department of Health and Human Services" ("OIG") has the authority to investigate information blocking. 42 U.S.C. § 300jj-52(b)(1). If, after "an investigation conducted under this subsection," the OIG finds that an entity engaged in information blocking, the OIG may impose "a civil monetary penalty determined by the Secretary." *Id.* § 300jj-52(b)(2). The OIG may also "refer such instances of information blocking to" HHS's Office for Civil Rights. *Id.* § 300jj-52(b)(3); *see also id.* § 300jj-52(d)(1). Additionally, an "entity … determined by the [OIG] to have committed information blocking shall be referred" for any applicable federal disincentives. *Id.* § 300jj-52(b)(2)(B).

B. Factual Background

1. PointClickCare provides valuable cloud-based healthcare software to healthcare providers.

PointClickCare is a Canadian technology company that provides state-of-the-art cloud-based software solutions in the EHI space. More than 30,000 healthcare providers use PointClickCare's proprietary SaaS platform as a secure means to organize, analyze, track, store, share, and exchange EHI for over 1.6 million patients. JA235 ¶ 5; JA289 ¶¶ 7-9; JA629 (Tr.254:2-10); JA682 (Tr.6:13-22). The platform allows patient-care teams to both input and retrieve a wide array of health information, including through PointClickCare-designed custom reports. JA289 ¶ 8; JA631-632 (Tr.256:22-257:5).

Data security is foundational to PointClickCare's ability to provide these services. PointClickCare complies with all requirements of HIPAA as amended by the HITECH Act, all the associated regulations, and all Canadian laws governing privacy and handling of EHI and personal health information. JA288 ¶ 5; *see* JA616 (Tr.271:22-25). As a leading EHI platform, PointClickCare has voluntarily certified compliance with standards, implementation specifications, and criteria adopted by the Secretary of the Department of Health and Human Services through the

Office of the National Coordinator for Health Information Technology ("ONC"). JA288-289 ¶ 6; JA629-630 (Tr.254:20-255:20). PointClickCare's ONC certification means that it meets the security, interoperability, and content standards required under Part 170 of the regulations. 45 C.F.R. Part 170. Importantly, that certification requires PointClickCare to provide USCDI version 1 data until January 1, 2026, when the content standard becomes USCDI version 3. *See* JA1155-1165.

2. PointClickCare's contracts govern its relationships with its customers.

PointClickCare's tens of thousands of healthcare-provider customers have contracts with PointClickCare to securely input, access, and share their patients' healthcare records. The contracts prohibit those customers from engaging in harmful activity that could slow the PointClickCare platform or open it to attack.

a. PointClickCare gives its customers many ways to access and share EHI. *See* JA289-291 ¶¶ 7-12; JA650-651 (Tr.275:24-276:5). Of particular relevance here are the following three.

First, under PointClickCare's master subscription agreements, customers can create user IDs for their authorized users to access PointClickCare's system. JA259-277; JA292 ¶ 18; JA636-637 (Tr.261:21-

262:11). When a user is logged in, the user can access EHI with modules and tools in the PointClickCare system. Users can also access various proprietary reports and download EHI in PDF format. JA289-290 ¶¶ 9-10; *see* JA637 (Tr.262:9-11).

Second, PointClickCare allows customers to access the federally standardized set of data elements through its "USCDI Connector" solution. JA289-290 ¶ 9; JA632 (Tr.257:6-8); JA1248-1254. USCDI—developed and maintained by ONC—is a uniform set of interoperable data elements required by Medicare and Medicaid. *See* ONC, Cures Act Final Rule—United States Core for Interoperability Fact Sheet, *available at* https://www.healthit.gov/sites/default/files/page2/2020-03/USCDI.pdf.

And *third*, PointClickCare allows its clients to seamlessly access third-party services through its "Marketplace" program. In the Marketplace program, PointClickCare has developed application programming interfaces ("APIs") that allow vetted and qualified third parties to integrate their software platforms directly with PointClickCare's system. JA252 ¶ 45; JA834 (Tr.158:5-10). This program allows PointClickCare's customers to share real-time access or analysis of electronic health information with approved business

associates. JA291 ¶ 12; JA834 (Tr.158:5-10). When third parties access PointClickCare systems via approved and controlled APIs, these third-party integration solutions allow PointClickCare to enforce security and performance safeguards—for example, allowing PointClickCare to temporarily cut off access to vendors infected with malware. JA252-253 ¶¶ 46-47; *see* JA787 (Tr.111:16-22). PointClickCare has working partnerships with well over a thousand third-party vendors and welcomes collaboration as long as the third-party vendor can be integrated in a way that maintains safety, security, and integrity of PointClickCare's systems and the data it stores. JA291 ¶ 14; JA631-632 (Tr.256:25-257:2); JA640-641 (Tr.265:14-266:2).

b. To protect the security and integrity of PointClickCare's systems and the sensitive EHI stored therein, the master subscription agreements restrict how PointClickCare's customers operate their accounts and access EHI. JA236-237 ¶¶ 11-12; JA638-640 (Tr.263:23-265:10).

Relevant here, the agreements explicitly prohibit customers from employing bots. As the district court explained,

> [t]he nursing facilities agree not to[] 'access the Services or allow any employee, contractor, or agent to access the

> Services, with, for example, *any automated or other process* such as screen scraping, by using robots, web-crawlers, spiders or any other sort of bot or tool, for the purpose of extracting data, monitoring availability, performance, functionality, or for any other benchmarking or competitive purpose.'

JA995 (emphasis added) (quoting JA203 § 2.2(x)). This across-the-board ban is contained in a section labeled "Prohibited Actions." JA203 § 2.2.

This restriction protects against two types of harm that bot usage can cause.

First, because of their ability to submit resource-intensive data requests much more rapidly than human users—and without the pause between actions that is natural for human users as they review information—bots can quickly overwhelm servers designed to accommodate human users, causing system slowdowns or even crashes, and preventing PointClickCare's customers from accessing EHI. JA240-243 ¶¶ 19-24; JA640 (Tr.265:6-10); JA640-641 (Tr.265:23-266:2).

PointClickCare manages its cloud storage space and allocates bandwidth based on its customers' anticipated usage. JA237 ¶ 15; JA686 (Tr.10:4-16); *see also* JA202-203. PointClickCare designed its systems to provide more than sufficient bandwidth to ensure system continuity when being accessed by human users consistent with its contracts.

JA237, JA254 ¶¶ 15, 52; JA686 (Tr.10:11-16). When a nursing home facility's resource limits are reached—which does not happen with normal human users—the facility cannot access patients' information until usage levels return to normal. JA242 ¶ 21; JA693-700.

Bots can pummel PointClickCare's system with rapid-fire requests for system-intensive tasks. JA238-243 ¶¶ 18-24; JA688 (Tr.12:8-16). Bots, for example, can demand excessive numbers of custom reports, which are generated on user demand. JA238-243 ¶¶ 18-24; JA688 (Tr.12:8-17). While a human user will require several moments to request a report, an automated bot can demand multiple reports per second. *See* JA692 (Tr.16:17-19). Generating reports is resource-intensive, and automated bot demands can overwhelm PointClickCare's storage and processing systems. JA243 ¶ 24. Moreover, every time certain patient reports are generated, HIPAA requires PointClickCare to generate accompanying audit reports, imposing additional system stress. JA243 ¶¶ 22-24. Skyrocketing bot use on PointClickCare's platform, including RTMS's bots, has led to outages and performance degradation. JA238-243 ¶¶ 18-22; JA688 (Tr.12:17-25). For example, one incident involving an RTMS bot user making excessive database queries caused a

system collapse impacting 10,000 patients, including 1,450 in Maryland. JA243 ¶ 24. Another bot incident resulted in database latency impacting 7,700 patients. JA243 ¶ 24.

The second risk posed by bots is a risk to EHI security, because bots are a vector for malicious cyberattacks. JA238 ¶ 18. Due to their automated nature and ability to make high-volume queries on systems, bots can be used to exfiltrate massive amounts of data, change code on the attacked platform, and even take over software platforms. *See supra* note 1. Cybercriminals who gain access to EHI may commit identity theft, sell the information, or prevent the EHI custodian from accessing the data unless the organization pays the thief a ransom. JA235 ¶ 8; JA687 (Tr.11:13-19). Cybercriminals may also manipulate data and alter the information in patients' medical records. Hacks of this nature in medical settings can have grave—even lethal—consequences. *See, e.g.*, Kim Zetter, *Hackers Can Send Fatal Dose to Hospital Drug Pumps*, Wired (June 8, 2015), https://tinyurl.com/yyctmkxu.

3. RTMS makes money by deploying bots on PointClickCare's system.

RTMS is a diagnostic-analytics company that primarily serves nursing homes. JA994. The company charges each client $400 to $500 a

month, promising to monitor their patients' EHI to identify medical changes and alert providers for intervention and preventative care. JA994; JA57 ¶ 16; JA606 (Tr.231:11-17). Many of RTMS's clients store their EHI on PointClickCare's platform.

RTMS has no licensing or data-sharing agreements with PointClickCare. *See* JA405 (Tr.30:2-4). Instead, RTMS asks its nursing home clients to create user credentials for RTMS on the client's account. JA403-404 (Tr.28:10-29:13); JA423 (Tr.48:5-9). RTMS then accesses PointClickCare's system with those credentials and deploys bots on the platform, where they initiate automated, rapid-fire requests for custom reports. JA58-60 ¶¶ 18-23; JA424 (Tr.49:7-17).

RTMS's use of bots violates PointClickCare's contractual ban. JA237 ¶ 13. By its own admission, RTMS employs bots because doing so increases its profit margin. Without bots, RTMS would have to hire and pay human employees to collect the data that fuels its business model, JA510, or contract for some other kind of access. RTMS's client fees (leaving aside other ways that it monetizes data) apparently yield an annual revenue stream of around $10 million. JA391-392, JA427 (Tr.52:1-2). And under its back-door bot arrangement, it gets the data it

monetizes for free: RTMS pays nothing for the access to PointClickCare's platform that it uses to exfiltrate EHI through bots running thousands of custom reports. As RTMS acknowledged, it would be reasonable for PointClickCare to charge it for that access. JA607.

4. PointClickCare elevated its security protocols to block all bots.

To protect the security of the patient health information with which it is entrusted, PointClickCare has deployed technological tools to enforce its contractual bot ban. *See* JA425 (Tr.50:5-7). Bots are a dynamic threat, so protecting against them requires flexibility to employ evolving technological defenses to respond to novel attack vectors. JA235-236 ¶¶ 6, 9.

Completely Automated Public Turing Tests to Tell Computers and Humans Apart ("CAPTCHAs") are the current industry-standard security measures for preventing bot use. JA244 ¶ 27; *see* JA702 (Tr.26:5-23). CAPTCHAs are well-known to Internet users and typically include puzzles that are challenging for computers to solve without human intervention—for example, requiring users to identify which images in an array contain a bicycle, or correctly type letters and numbers displayed in a skewed image. *E.g.*, JA479 (Tr.104:2-5); *see*

JA247-249 ¶¶ 35-37 (other CAPTCHA examples); JA1109, JA1110. Since 2022, PointClickCare has used CAPTCHAs to block high-volume bot users from accessing its systems and has adjusted them to respond to increasingly sophisticated technologies, like image-recognition software, that enable bots to defeat more rudimentary CAPTCHA tests. JA244-246 ¶¶ 27-33; JA702-703 (Tr.26:24-27:1). RTMS admits that it defeated PointClickCare's CAPTCHAs by having humans log in and then deploying bots. JA448-449 ("[W]e have humans that solve those.").

PointClickCare most recently updated its CAPTCHA technology in May 2024 to make the CAPTCHAs more effective at permanently blocking user IDs deploying high-volume bots. JA715 (Tr.39:16-24). When PointClickCare detects that a user is demanding at least 10–20 times more data than an average human user and thus likely employing a high-volume bot, PointClickCare places the affected user ID on a watch list. JA704 (Tr.28:12-20); JA724 (Tr.48:2-16). Those watch-listed user IDs must solve increasingly difficult CAPTCHAs. *See* JA705 (Tr.29:11-13); JA717-718 (Tr.41:18-42:3). Once PointClickCare has high confidence that the user ID is being used by bot (so as to not block legitimate users), it presents an indecipherable CAPTCHA, effectively blocking that user

ID from accessing PointClickCare's platform. *See* JA718 (Tr.42:12-24). Once blocked, a user must contact the client to obtain a new user ID. JA553 (Tr.178:7-14).

5. PointClickCare and RTMS negotiated possible commercial solutions but could not reach agreement.

PointClickCare and RTMS explored a merger in 2023. *See* JA583 (Tr.208:12-20). After merger discussions stalled, the parties considered a strategic partnership that would enable RTMS to acquire data from PointClickCare's system through a negotiated custom API instead of through RTMS's existing bots that breach PointClickCare's contracts and overwhelm PointClickCare's platform. JA 587-588 (Tr.212:20-213:2). Around October 2023, PointClickCare provided RTMS with its standard Marketplace Partner Agreement, which would enable RTMS to access patient data in the same way as more than one thousand other third-party vendors. JA326 ¶ 4. As with PointClickCare's client agreements, the Marketplace agreement bars the vendor from using bots on PointClickCare's system. JA326 ¶ 4. RTMS rejected the proposed agreement, returning a redline that struck the provisions barring bot access and greatly reduced the amount it would pay PointClickCare,

among other changes. *See* JA340-359; JA592 (Tr.217:2-10). RTMS's refusal to accept the bot prohibition applicable to all other Marketplace vendors ended those discussions. JA842-848.

PointClickCare does not own the EHI stored on its platform. In fact, PointClickCare's customer contracts explicitly reject any ownership claim. JA326 ¶ 5. And RTMS's status as a competitor to some aspects of PointClickCare's business would not prevent PointClickCare from entering into a mutually agreeable strategic solution. JA326-327 ¶ 6. PointClickCare contracts with several other companies that offer services similar to RTMS's. *See* JA646 (Tr.271:7-15). PointClickCare has repeatedly engaged with RTMS in efforts to find a commercial solution that will provide RTMS with the data the company wants. JA326-327 ¶ 6. But PointClickCare will not provide access through a means that jeopardizes its data security and platform functionality. JA326-327 ¶ 6.

RTMS—through its customers' logins—may acquire data using individual patient queries requested by human users, as every PointClickCare customer is authorized to do. Or RTMS could negotiate to use the USCDI Connector or other access. Or RTMS could join the Marketplace program and access the data through a custom API if it were

willing to fairly compensate PointClickCare for that buildout. But that is not enough for RTMS—it wants *all* the data it demands, for free, using bots.

C. Procedural Background

This Suit. RTMS sued PointClickCare in January 2024, asserting numerous causes of action, most of which focused on PointClickCare's efforts to secure its platform. PointClickCare moved to dismiss, and that motion remains pending. On May 30, 2024, RTMS moved for a preliminary injunction, and an evidentiary hearing was held June 24 and 25, 2024.

The Evidentiary Hearing. At the hearing, both sides presented witnesses and exhibits. JA683 (Tr.7:17-25); JA684 (Tr.8:1-15); JA711 (Tr.35:19-25); JA712 (Tr.36:1-25). Even though the hearing concerned RTMS's motion seeking extraordinary relief, the district court imposed a much heavier evidentiary burden on PointClickCare than on RTMS. For example, the district court accepted as true a single witness's assertion, unsupported by any documentary evidence, that RTMS would go out of business if PointClickCare limited or blocked bot access. JA611 (Tr.236:7-10). On the other hand, the court rejected testimony from

Bachar Fourati, PointClickCare's head of SaaS platform operations, that bots cause outages on its system—even though *that* testimony *was* backed with documentary evidence, including documentation of an outage caused by an RTMS bot. The court rejected PointClickCare's evidence, moreover, despite RTMS proffering *no* contrary evidence on that point. *See* JA505 ("Q. So you're unable to assess the actual impact that any bots have had on [PointClickCare's] system, correct? A. Correct." (cross-examination of Christopher Miller, RTMS Chief Technology Officer)).

In another example, the court grilled Mr. Fourati about PointClickCare's bot-blocking procedures. The court repeatedly pressed Mr. Fourati for an "objective" trigger that led to blocking. Fourati provided that objective trigger: 15 to 20 times the usage of a normal user. JA770. He estimated that a normal human user's maximum volume is in the range of 500 to 1,000 queries per day. JA771. PointClickCare accordingly places user IDs on the watch list when they issue queries at a rate equivalent to generating 15,000 queries per day. Inexplicably, the court ignored testimony about that threshold, which was clearly in the

record. *See* JA1002 ("PCC … offered no objective criteria for what lands a user ID on the watch list").

Relatedly, the court accepted a single RTMS witness's word—again, unbacked by any document—that RTMS could not operate *at all* when *some* of its bots were blocked. JA1005. Yet when Mr. Fourati testified that PointClickCare applied its watch list uniformly, the court demanded documentary evidence. PointClickCare, with only a few minutes' notice, provided the court with the then-current watch list, showing that only a fraction of the blocked users were associated with RTMS. JA1532-1547. Yet the court rebuffed that unrebutted evidence too.

The Preliminary Injunction. The district court granted RTMS an injunction on July 29, 2024, prohibiting PointClickCare from using the bot-blocking CAPTCHAs against RTMS user IDs. JA994. The court ruled that RTMS was likely to succeed on both its unfair-competition and tortious-interference claims. JA1006. The court held that PointClickCare's use of CAPTCHAs constituted information blocking in violation of the Cures Act and did not fall within any of three enumerated exceptions to the Act's definition of information blocking—the health IT

performance exception, the security exception, and the manner exception. JA1008.

The court concluded the health IT performance exception was not applicable because PointClickCare did not prove that RTMS's use of bots "meaningfully" impacts system performance, that CAPTCHAs are deployed no longer than necessary to resolve any negative impacts, or that unsolvable CAPTCHAs are used in a consistent and nondiscriminatory manner. JA1008-1010. Similarly, it held that the security exception was not applicable because PointClickCare failed to prove that the use of CAPTCHAs is directly related to safeguarding EHI, tailored to a specific security risk, and used in a consistent and nondiscriminatory manner. JA1008-1012. And the court held that the manner exception did not apply because PointClickCare did not prove that there are no agreeable terms for an alternative—a judicially created burden that does not appear in the regulation. JA1012-1013.

Regarding the tortious-interference claim, the court concluded that RTMS showed that PointClickCare's use of CAPTCHAs intentionally interfered with its performance of its contracts with skilled nursing facilities. JA1015-1016. The court reasoned that PointClickCare knew

about RTMS's contractual relationships with nursing facilities, that PointClickCare prevented RTMS from accessing patient records necessary to fulfill its contracts, and that RTMS suffered damages as a consequence. JA1015-1016. The court then found that RTMS would suffer irreparable harm and that the balance of equities and public interest weighed in favor of granting the injunction. JA1017-1018.

This appeal followed.

SUMMARY OF ARGUMENT

I. Both state-law claims on which the district court based its injunction order are premised on the proposition that PointClickCare violated the Cures Act by blocking bots. But under the Cures Act's manner exception, PointClickCare may deny access to RTMS's bots so long as it is willing to provide the standardized access federal regulations require—which PointClickCare does. Moreover, the court's error in turning the injunction-stage burden of proof on its head meant it was wrong when it ruled PointClickCare's actions were not authorized by the Cures Act's exceptions for blocking harmful third-party applications and for preserving EHI security. The district court's misinterpretation of the Cures Act raises grave constitutional concerns because it effects a taking

of PointClickCare's property without compensation, further demonstrating that the district court erred as a matter of law.

II. RTMS's state-law claims are likely to fail for other, independent reasons. The Cures Act is enforced by a federal agency and provides no private right of action. RTMS's attempt to manufacture one by using purported violations as a predicate for state-law claims is improper, as was the district court's acceptance of that stratagem. RTMS's tortious-interference claim must fail, moreover, because PointClickCare's evenhanded actions barred *all* users from employing bots and were not directed to RTMS alone.

III. The district court also misapplied the remaining preliminary injunction factors. Instead of requiring RTMS to show that it would suffer irreparable harm, the district court accepted RTMS's *ipse dixit* assertion that it would go out of business—instead of just suffer economic injury, which cannot constitute irreparable harm—if PointClickCare employed industry-standard security protocols to block bots. In fact, RTMS acknowledged that it could employ humans to perform the same tasks—a harm that, by definition, is not irreparable because it is compensable by monetary damages. Nor did the district court correctly

balance RTMS's alleged harm against PointClickCare's evidence that the injunction poses existential risks to PointClickCare and its customers' patients. And the public has a strong interest in proper enforcement of the laws governing EHI interoperability, security, and privacy.

LEGAL STANDARD

The district court's decision whether to grant a preliminary injunction is reviewed for an abuse of discretion, such as a mistake of law. *Quince Orchard Valley Citizens Ass'n, Inc. v. Hodel*, 872 F.2d 75, 78-79 (4th Cir. 1989). "A district court abuses its discretion when it misapprehends or misapplies the applicable law," so its legal conclusions are reviewed *de novo*. *League of Women Voters v. North Carolina*, 769 F.3d 224, 235 (4th Cir. 2014).

A preliminary injunction is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008). To warrant a preliminary injunction, a party must demonstrate that: (1) it is likely to succeed on the merits; (2) it is likely to suffer irreparable harm in the absence of relief; (3) the balance of equities tips in its favor; and (4) an injunction is in the public interest. *Id.* at 20.

This Court reviews *de novo* which party bears the burden of proof. *See Everett v. Pitt Cnty. Bd. of Educ.*, 678 F.3d 281, 288 (4th Cir. 2012).

ARGUMENT

I. The Preliminary Injunction Must Be Set Aside Because PointClickCare Complies With The Cures Act.

The district court rested its decision on the faulty premise that the Cures Act requires PointClickCare to let RTMS use bots to access its platform. This was an error because enforcing contractual provisions that prohibit bots is a "reasonable and necessary" activity that "do[es] not constitute information blocking," 42 U.S.C. § 300jj-52(a)(1), (a)(3), under each of three exceptions—for manner, IT performance, and security. And the court's opinion mandating that PointClickCare provide RTMS unlimited, free access to PointClickCare's system raises serious constitutional issues. Because the district court "misapprehend[ed] … the applicable law" in its "likelihood of success on the merits" analysis, it abused its discretion. *League of Women Voters*, 769 F.3d at 235, 238.

A. Both of RTMS's causes of action are premised on violations of the Cures Act.

Although RTMS pressed three claims as bases for its preliminary injunction—"tortious interference with business relations, unfair competition, and breach of contract as a third-party beneficiary"—the

district court addressed only the first two. *See* JA1006. But all three claims rise or fall with RTMS's misguided allegations that PointClickCare violated the Cures Act.

Under Maryland law, an unfair-competition claim enforces "the general principle that all dealings must be done on the basis of common honesty and fairness, without taint of fraud or deception." *Balt. Bedding Corp. v. Moses*, 34 A.2d 338, 342 (Md. 1943). Here, what RTMS alleges is unfair is the purported violation of the Cures Act. JA40-41 ¶¶ 132-34.

Similarly, RTMS's tortious-interference claim requires it to show "that the actions undertaken were 'wrongful,'" *Baron Fin. Corp. v. Natanzon*, 471 F. Supp. 2d 535, 541 (D. Md. 2006) (quoting *Martello v. Blue Cross & Blue Shield of Md., Inc.*, 795 A.2d 185, 193 (Md. Ct. Spec. App. 2002)). The wrongful conduct RTMS alleges to support its tortious-interference claim is, again, the purported violation of the Cures Act. JA43-44 ¶¶ 153-54. This dispute, and the court's injunction, thus hinge on PointClickCare's compliance with the Cures Act.

B. PointClickCare offered RTMS more access to data than the Cures Act requires after the parties failed to come to an agreement on data transfers.

RTMS's human users had full access to all information that RTMS claims to need. *E.g.*, JA423, JA488, JA503. The only dispute was over the manner in which RTMS can access that information—*i.e.*, whether the Cures Act absolutely entitles RTMS to use high-volume bots to siphon data from PointClickCare's platform. PointClickCare's customers agree to a contractual prohibition against using bots on its system. RTMS, which has no legal right to use login credentials to access PointClickCare's system except as a delegate of a PointClickCare customer, is required to adhere to the same terms as PointClickCare's customers and to access the system with human users. RTMS, a nonparty to any relevant agreement with PointClickCare, has no special dispensation under the Cures Act to use its own nonstandard manner of access via bots.

Under the manner exception, whenever the custodian "cannot reach agreeable terms with the requestor to fulfill the request in the manner requested," any "practice of limiting the manner in which" a custodian "fulfills a request to access, exchange, or use" EHI is not

information blocking so long as the custodian provides alternative access through approved, standardized methods. 45 C.F.R. § 171.301(a)(1) & (b). Here, PointClickCare and RTMS could not reach agreeable terms to fulfill RTMS's request to run bots. PointClickCare offered approved alternative means of providing EHI, but RTMS rejected that offer.

The parties sought to negotiate a commercial resolution. JA999-1000. Acknowledging that its activity is costly and taxing on PointClickCare's system, RTMS offered to pay $70 per month per facility for permission to deploy its bots. JA413-414 (Tr.38:16-39:2); JA596-597 (Tr.221:23-222:3). Multiplying that number by 1500 facilities, this would amount to $105,000 a month or $1.26 million a year. *See* JA597 (Tr.222:4-7). But because bot use is unacceptable, PointClickCare countered by offering RTMS access through a Marketplace API for $65 a month, or $125 a month for a premium API. *See* JA596-597 (Tr.221:25-222:7). RTMS then offered less than 50% of what PointClickCare requested—$30 a month to join Marketplace or $60 a month for the premium model. JA597 (Tr.222:14-16).

In addition to the parties' inability to reach agreement on price, RTMS refused to comply with PointClickCare's bot prohibition. *See*

JA343-344 ¶ 2.8 (RTMS redline) (seeking the right to access PointClickCare's systems "with an automated or other process or tool, for the purpose of extracting data"); JA345 ¶ 3.10 (adding exception to blanket prohibition on the use of "any automated or other process such as robotic process automation"); *see also* JA494-495. The parties did not reach an agreement. *See* JA1000.

Because the parties could not reach mutually agreeable terms, the regulation allows PointClickCare to "fulfill the request in an alternative manner." 45 C.F.R. § 171.301(b)(1). PointClickCare can do this in multiple ways. It could offer RTMS: (1) "technology certified to standard(s) adopted in part 170," (2) data using "content and transport standards … published by" the federal government or an ANSI-accredited standards organization, or (3) data in "an alternative machine-readable format … agreed upon with the requestor." *Id.* § 171.301(b)(1)(i)-(iii).

PointClickCare complied with those requirements. First, PointClickCare's systems are certified to standards HHS adopted in part 170. *See* JA288-289 ¶ 6; JA630; *see also* JA532-534, JA641-642. Accordingly, RTMS's undisputed access to those systems satisfied the

first alternative-manner prong. *See* 45 C.F.R. § 171.301(b)(1)(i). Second, PointClickCare made data available to RTMS in USCDI v.1 format through its USCDI Connector offering. *See* JA289-290 ¶ 9; JA325-326 ¶ 3; JA631. That is the "content and transport standards … published by" the federal government. 45 C.F.R. § 171.301(b)(1)(ii)(A); 45 C.F.R. § 170.213; JA1173 (noting that ONC's USCDI version 1 is the applicable content standard under part 170 until January 1, 2026).

PointClickCare fully satisfied the manner exception by offering data to RTMS in those two standardized alternative manners. (Moreover, RTMS undisputedly has access through human users to all the data it wants.) Offering "at least two alternative manners in accordance with § 171.301(b)" exhausts the manner exception. 45 C.F.R. § 171.204(a)(4). And "not fulfilling a request to access, exchange, or use" EHI when the manner exception has been exhausted is not information blocking. *See id.* § 171.204(a)(4).

These undisputed facts should have been the end of the case. The parties could not agree on terms, so PointClickCare offered the alternatives required by law and thereafter had no further obligation to RTMS under the Cures Act. But the district court ignored the regulation

and manufactured its own standard instead, under which negotiations needed to continue until PointClickCare let RTMS do what it wanted. According to the district court, the fact that the parties could not agree on terms "does not suggest that PCC can find no 'agreeable terms.'" JA1013. This conclusion conflicts directly with the regulation's text.

The manner exception applies when "the actor … cannot reach agreeable terms with the requestor." 45 C.F.R. § 171.301(a). The regulation does not authorize a judge to decide which terms a custodian (or requestor) must find agreeable—*i.e.*, to perform the parties' contract negotiation in the parties' stead. Instead, the word "agreeable" means "able to be accepted by everyone." Cambridge Dictionary (2024), https://tinyurl.com/4pv735m3. Neither party found the other party's terms agreeable. If a term must be "agreeable" to two parties, then "agreement of both parties … [is] required." *Ross Grp. Constr. Corp v. Riggs Contracting, Inc.*, 2012 WL 5511644, at *6 (N.D. Okla. Nov. 14, 2012). Terms not agreed are self-evidently not *agreeable* to at least one party.

The district court misconstrued the phrase "cannot reach agreeable terms" to mean that the manner exception is available only when a party

is "unable" to reach agreement, and that the exception is unavailable if, *in the court's opinion*, a party is merely "unwilling" to reach agreement. JA1012-1013. But parties often "cannot reach agreeable terms" because one or the other is *unwilling* to do so. *E.g.*, *Peyton v. Reynolds Assocs.*, 955 F.2d 247, 249, 253 (4th Cir. 1992) (affirming grant of summary judgment to a defendant that was "unwilling to agree to some of the terms" in a contract). The court's limitation of the phrase "cannot reach agreeable terms" to include only those situations in which parties are "unable" to reach agreement imposes a duty to agree wherever agreement is technically possible, no matter how onerous the counterparty's demands—a condition the district placed only on PointClickCare. In other words, the district court improperly narrowed the regulatory language's scope.

The district court's reading is also inconsistent with the obvious intent of the regulation, which is to provide a safe harbor for custodians that share *at least* the federally mandated baseline for EHI data sharing. 45 C.F.R. § 171.301(a) & (b). The district court's construction yields an absurd result that turns half the regulation into surplusage: the custodian will never be able to avail itself of the regulation's specified

safe harbor of providing EHI according to the federal baseline. *See United States v. Simms*, 914 F.3d 229, 241 (4th Cir. 2019) (rejecting "reading[s] … that render[] part of the statute superfluous"). Instead, the requestor can make unreasonable demands and obtain an injunction requiring the EHI custodian to acquiesce to its terms. Moreover, an EHI provider later deemed by a judge to have been "unwilling" but not technically "unable" to find the requester's demands "agreeable" could be exposed to monetary sanctions imposed by the OIG. 42 C.F.R. § 1003.1410; *see generally* HHS OIG, *Information Blocking* (Sept. 14, 2023), https://tinyurl.com/2xj7jhsc.

The district court's interpretation cannot be squared with HHS's explanation of the language of the manner exception, which aligns with its ordinary meaning. *See Kisor v. Wilkie*, 588 U.S. 558, 570 (2019) ("The agency that 'wrote the regulation' will often have direct insight into what the rule was intended to mean."). As HHS explained, the manner exception "allow[s] actors [*i.e.*, custodians like PointClickCare] to first attempt to negotiate agreements in any manner requested with whatever terms *the actor* chooses." 85 Fed. Reg. at 25,877 (emphasis added). And "if the actor cannot reach agreeable terms with the requestor to fulfill the

request," the actor may then "satisfy the exception by fulfilling the request in an alternative manner." *Id.* Making clear that the district court had the law backward, HHS provides an example showing that PointClickCare need not accept RTMS's terms before offering the data via one of the alternative formats:

> For instance, under the exception, actors who cannot reach agreeable terms with the requestor to fulfill the request are *not* required to license their IP to proprietary technology in order to satisfy the exception.

Id. The key goal is to "allow[] the actor enough flexibility to avoid developing one-off, unique, custom solutions *unless the actor wants to do so*." 89 Fed. Reg. 1192, 1384 (Jan. 9, 2024) (emphasis added).

That is precisely the situation PointClickCare faced. Despite being able to access all the data it needs with human users, RTMS demands nonstandard, unlimited bot access to PointClickCare's system and wants to continue paying PointClickCare nothing, or at most less than PointClickCare asks (and less than its Marketplace-program partners pay for safe and secure integrated access). The Cures Act does not require PointClickCare to develop a "one-off, unique, custom solution[]" for RTMS on those terms. *Id.* at 1384. What the district court granted RTMS was in essence a compulsory license to PointClickCare's SaaS

platform, contradicting the regulation establishing that PointClickCare is "*not* required to license" its proprietary system to RTMS to satisfy the manner exception. 85 Fed. Reg. at 25,877.

C. PointClickCare's security protocols are also protected by the IT performance and security exceptions.

PointClickCare's anti-bot protocols are reasonable and necessary and thus do not constitute information blocking under the IT performance and security provisions of the Cures Act. The district court made legal errors in finding otherwise, including placing the burden of proof on PointClickCare.

1. The court misapplied the burden of proof.

The district court repeatedly misconstrued and misapplied the burden of proof. At the preliminary-injunction stage, the plaintiff's burden is not just to prove its case by a preponderance of the evidence; it must make an elevated "clear showing" of entitlement to relief. *Winter*, 555 U.S. at 22. The district court failed to hold RTMS to that standard, and then enforced disparate burdens, demanding PointClickCare produce exacting evidence. *See supra* pp. 23-25. And the court further required PointClickCare to prove it was abiding by the Cures Act, when in fact RTMS bore the burden to satisfy the elements of its state-law

claims, which required proving that PointClickCare was acting unlawfully. *Winter*, 555 U.S. at 22. All those are reversible errors. *Humphrey v. Humphrey*, 434 F.3d 243, 247 (4th Cir. 2006) (improperly heightened burden of proof is a "serious [error] because the proper allocation of the burden of proof is an important procedural right." (cleaned up)).

The plaintiff's burden is to show it is likely to succeed in proving each element of its claim. *Gonzales v. O. Centro Espirita Beneficente Uniao do Vegetal*, 546 U.S. 418, 428 (2006); *Roe v. Dep't of Def.*, 947 F.3d 207, 224 (4th Cir. 2020), *as amended* (Jan. 14, 2020). Both state-law claims on which the district court relied were premised on alleged violations of the Cures Act. *See* JA1007; *supra* part I.A. As the moving party, RTMS had the burden to show that PointClickCare in fact violated the Cures Act by acting inconsistently with the regulatory definition of information blocking promulgated by HHS. Such a showing would be "necessary to establish the very illegality of the behavior." *United States v. Hooker*, 841 F.2d 1225, 1231 (4th Cir. 1988) (quotation marks omitted).

RTMS made no such showing. Instead of holding RTMS to its burden, the court shifted the burden at each turn and held that

PointClickCare had not introduced sufficient evidence to establish that its conduct was lawful. *See, e.g.*, JA1010 ("On this record, the Court cannot conclude that PCC deploys its CAPTCHAs in an even and nondiscriminatory manner"); JA1012 ("PCC cannot invoke the security exception."); JA1013 ("the Court cannot conclude that PCC is 'technically' unable to fulfill Real Time's requests for records"). But the issue is not whether PointClickCare proved that it behaved lawfully. Instead, it is whether RTMS proved that PointClickCare likely *violated state law* by acting outside the scope of the "reasonable and necessary" activities identified by HHS under the Cures Act.

Showing that a custodian's activities fall outside the scope of the reasonable and necessary activities HHS identified is an essential element of a Cures Act violation. The Cures Act defines which activities constitute information blocking and which activities do not. Congress recognized the importance of "identify[ing] reasonable and necessary activities *that do not constitute information blocking*" and tasked HHS with promulgating regulations identifying those activities. 42 U.S.C. § 300jj-52(a)(3) (emphasis added). Accordingly, an EHI custodian's actions are "not information blocking"—and do not violate the Cures

Act—unless they are not among the "reasonable and necessary" activities HHS identified. Because RTMS failed to prove that PointClickCare's conduct fell outside these activities, RTMS has not established a likelihood of success on the merits.

2. The Cures Act authorizes PointClickCare to block bots to protect the performance of its IT systems.

HHS recognizes that there are "circumstances [in which] it may be appropriate for actors to take action (*e.g.*, deny access, throttle, or meter) to limit the negative impact on the performance of health IT that may result from the technical design, features, or behavior of a third-party application." 85 Fed. Reg. at 25,874. It accordingly tailored subsection (b) of the health IT performance exception to the information-blocking rule for precisely the situation PointClickCare faced. Under that subsection, it is not information blocking to "take action against a *third-party application* that is negatively impacting the health IT's performance," 45 C.F.R. § 171.205(b) (emphasis added), including by "deny[ing] access" to the third party's application, 85 Fed. Reg. at 25,874. That action is not information blocking as long as it is: (1) imposed for no longer than necessary to resolve the negative impacts, (2) implemented

in a consistent and nondiscriminatory manner, and (3) consistent with existing service-level agreements. *Id.*

The district court's failure to require RTMS to bear the burden of proof on these issues is fatal to its decision. PointClickCare introduced evidence that high-volume bot usage *always* negatively impacted its system's performance. *See* JA238-242 ¶¶ 18-20 & charts cited (JA1092, JA1093, JA1097, JA1098). As the district court acknowledged, the evidence showed "bot-related performance problems" that "are tied to PCC's available server space." JA1003. Accommodating bot activity, the court explained, would require PointClickCare to "purchas[e] more server space" than is needed for the human use contemplated by PointClickCare's contracts. JA1003.

The court further noted that there was evidence tying bot-related performance problems to RTMS, explaining that PointClickCare offered a chart showing that "data retrieval from one nursing facility was slow, which it attributed to Real Time's contemporaneous use of automated data retrieval software." JA1003 (quotation marks omitted). RTMS offered no credible contrary evidence. *See* JA505 (RTMS was "unable to assess the actual impact that any bots have had on [PointClickCare's]

system"). PointClickCare implemented a policy that blocked users whose accounts repeatedly showed bot activity. JA234-256, JA1099-1106. And it applied that policy across the board to all such accounts—whether they belonged to RTMS or not. In fact, of approximately 600 user IDs PointClickCare placed on its watch list because of bot activity, only 119 were RTMS users. JA711-712.

Despite this lopsided evidence, the district court still enjoined PointClickCare's protocols. The court claimed that because of the "size of [PointClickCare's] own operations," it "[could] not simply take [PointClickCare's] word for it that automated software use … makes a material difference in PCC's performance." JA1009. In particular, the court asserted that PointClickCare offered "no evidence that Real Time's activities are even associated with slowdowns *beyond a single day*." JA1009 (emphasis added). At the rushed evidentiary hearing,[2] PointClickCare introduced evidence of the impact during a single day as an example of bot usage. The district court's assertion that evidence

[2] The district judge began the first day of the evidentiary hearing by emphasizing that she wanted "to get it done today." JA382 (Tr.7:15-16).

before it did not exist is clearly erroneous. JA238-242 ¶¶ 18-20 (highlighting instances when RTMS bots caused system slowdowns).

Nor is the district court correct in its insinuation that PointClickCare could only show that there was "meaningful[] impact[]" on PointClickCare's system performance by showing "complete system outages." *See* JA1009. The regulation imposes no such requirement. All that is needed is a showing that the third-party application "negatively impact[s] … performance" of a health IT system. 45 C.F.R. § 171.205(b). That low bar reflects the fact that this exception concerns blocking *third-party* applications—software with which the health IT system was not designed to interact and that might have unexpected deleterious effects on that system. PointClickCare's evidence clearly showed such a "negative[] impact" from RTMS's bots.

And the district court was incorrect in concluding that PointClickCare failed to limit the "use[] [of] unsolvable CAPTCHAS for no longer than is necessary to resolve any negative impacts." JA1009-1010. Because high-volume bot users' nonstandard access *always* has a negative impact on performance, preventing that effect requires

permanently blocking *all* bots by prohibiting accounts associated with bot use.

Finally, the IT performance exception requires that protocols be "implemented in a consistent and nondiscriminatory manner." 85 Fed. Reg. at 25,874. The injunction prevents PointClickCare from doing that by mandating preferential treatment for RTMS's bots.

3. PointClickCare is authorized by the Cures Act to block bots to mitigate security risks.

PointClickCare's bot-blocking actions—including the bot-blocking CAPTCHAs—also satisfied the security exception to information blocking. *See* 45 C.F.R.§ 171.203. That exception applies to practices that relate directly to safeguarding the confidentiality, integrity, and availability of EHI; that are tailored to a specific security risk; and that are implemented consistently and in a non-discriminatory fashion. *Id.* § 171.203(a)-(c). In addition, the practice must either (1) implement a written organizational security policy that aligns with best practices, or (2) be necessary to mitigate the security risk posed by the prohibited access, with no reasonable alternative methods available that are less likely to interfere with EHI access. *Id.* § 171.203(d), (e).

Bots pose significant security risks. As PointClickCare explained, malicious bots can be used to exfiltrate massive amounts of data, incorrectly change medical information, and cause PointClickCare's system to malfunction, which all pose unacceptable risks. JA687 (Tr.11:13-25); JA237 ¶ 14; JA1529-1531. And PointClickCare cannot tell whether bots are malicious or not. *All* bots are contractually prohibited. Further, customers manage their own user IDs—so PointClickCare does not provide user IDs to RTMS. RTMS instead uses PointClickCare customers' user IDs. Accordingly, PointClickCare has no way of knowing whether a bot slowing its system is doing so maliciously—or just recklessly, like RTMS's. *See* JA710 (Tr. 34:8-11) (noting that before the litigation, PointClickCare did not know which user IDs were associated with RTMS). And hackers can engage in spoofing where they pass themselves off as valid user IDs with normal IP addresses. JA385-386 (Tr.10:23-11:10). That is why, when PointClickCare detects bot activity, it must act to block the threat to its system.

Worse still is the risk to patients' EHI. PointClickCare designs its systems for use by healthcare providers, who need to be able to update patients' EHI with new information. When RTMS employs bots on

PointClickCare's system, RTMS uses login IDs designed for human users. *See* JA503. If those logins have the authority to modify or even delete patient records, a bot programmed maliciously—or even negligently—could wreak havoc.

PointClickCare's customers who contract with RTMS control whether the logins they give RTMS have permissions to alter patient EHI stored on PointClickCare's system. RTMS concedes it *doesn't know* whether particular login IDs that its bots use have the ability to alter data on PointClickCare's system. JA504-505. RTMS also cannot know whether a bot deployed by RTMS modifies patient data on PointClickCare's systems as a result of misconfiguration or an unexpected interaction with PointClickCare's software.

That is one of the numerous reasons PointClickCare bans bots on its system and employs CAPTCHAs to keep them off: doing so keeps the EHI on its system confidential, protects its integrity, and ensures that the EHI remains available on demand to its customers. *See* 45 C.F.R. § 171.203(a). CAPTCHAs are an industry-recognized anti-bot tool; indeed, their anti-bot purpose is clear from their name—tests to tell *computers and humans apart*. JA244 ¶ 27; *see also* JA996. Accordingly,

their use is tailored to the specific security risks posed by bots. *See* 45 C.F.R. § 171.203(b). And PointClickCare uses CAPTCHAs against *all* accounts that show high-volume bot activity—not just those operated by RTMS. JA712; *see* 45 C.F.R. § 171.203(c).

The district court quibbled that "[l]eft unanswered [during the brief evidentiary hearing permitted by the court] … was why PCC chose to implement unsolvable CAPTCHAs." JA1004. But that is a question RTMS itself answered. As PointClickCare explained, it placed an account on a watch list and presented CAPTCHAs only after it observed clear evidence of prohibited bot activity. JA704-705. But as the district court noted, RTMS found a way around those CAPTCHAs: "Real Time … previously navigated PCC's … CAPTCHAs by having humans sign into PCC's platform." JA998; *see* JA448-449 ("[W]e have humans that solve those."). Once its user logged in, RTMS again deployed its bot on that account. JA446-447.

To stop RTMS from circumventing its anti-bot security measures, PointClickCare employed indecipherable CAPTCHAs as the last step to lock out a user ID after its behavior showed that it was being used by a bot. In other words, RTMS's own behavior evading the restrictions

PointClickCare imposed to prevent unauthorized access made the employment of indecipherable CAPTCHAs "necessary to mitigate the security risk" RTMS's bots posed, and left PointClickCare with no "reasonable and appropriate alternatives" to the practice. 45 C.F.R. § 171.203(e)(1) & (2).

* * * *

PointClickCare's standard contract with all its customers prohibits the use of bots on PointClickCare's system. It enforces that ban in a variety of ways, including through CAPTCHAs that ultimately block accounts used by bots. Neither the ban nor its implementation violates the Cures Act. PointClickCare offered RTMS multiple alternative means of accessing EHI, but RTMS declined. Federal law requires no more.

D. The district court's misinterpretation of the Cures Act raises grave constitutional questions.

Under the "constitutional-avoidance canon, when statutory language is susceptible of multiple interpretations, a court may shun an interpretation that raises serious constitutional doubts and instead may adopt an alternative that avoids those problems." *Jennings v. Rodriguez*, 583 U.S. 281, 286 (2018). The court's duty is to "seek harmony, not to manufacture conflict," so the court should adopt any "fairly possible"

interpretation of the statute that avoids constitutional concerns. *United States v. Hansen*, 599 U.S. 762, 781 (2023).

Here, the district court's interpretation of the Cures Act invades a number of interlocking property interests PointClickCare owns in its systems and software. *First*, and most basically, PointClickCare has a property interest in its computer systems. The right to exclude others is a fundamental property right. *E.g.*, *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 149 (2021) ("The right to exclude is one of the most treasured rights of property ownership.") (quotation marks omitted). And both federal and Maryland law recognize that owners of computer systems have a right to exclude unauthorized users from accessing those systems. Like trespassing on real property, trespassing on computer systems is a crime. 18 U.S.C. § 1030; Md. Crim. Code § 7-302.

By preventing PointClickCare from using effective means to exclude RTMS's bots from PointClickCare's systems, the district court's injunction amounts to a taking of PointClickCare's property right to exclude. It is no answer to say that the general purpose of the Cures Act is to advance interoperability and increased access to EHI. Just as the owner of a public-facing shopping mall may be required to open its doors

to the public but can enforce generally applicable rules, for example, barring the use of dirt-bikes on the premises or setting the hours the premises is open, PointClickCare may choose to prohibit third parties from running harmful automated software on its system.

Second, access to PointClickCare's SaaS platform is governed by its master subscription agreements with its customers. JA994-995; *see* JA236 ¶ 11. Among the rights PointClickCare bargains for in those agreements is the right to keep its system free from "robots, web-crawlers, spiders or any other sort of bot or tool, for the purpose of extracting data." JA995 (quoting JA203 § 2.2); JA260. And "[c]ontract rights are a form of property" subject to the Fifth Amendment's restrictions on takings. *U.S. Tr. Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977). The district court's misinterpretation of the Cures Act strips PointClickCare of the contractual right it negotiated.

Third, although PointClickCare doesn't own patients' EHI, it owns copyrights in the selection and arrangement of data elements on its custom reports. *See Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 348 (1991) ("[C]hoices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal

degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws."). "An interest in a copyright is a property right protected by the … just compensation clause[] of the Constitution." *Roth v. Pritikin*, 710 F.2d 934, 939 (2d Cir. 1983). The district court's interpretation of the Cures Act requires PointClickCare to continue giving RTMS free and unlimited copies of its copyrighted arrangements in derogation of PointClickCare's exclusive rights under the Copyright Act. *See* 17 U.S.C. § 106(1).

If the Cures Act requires that a requestor receive carte blanche to invade these property interests, as the district court apparently believed, then the Act represents an unconstitutional taking of PointClickCare's property without just compensation. *See* U.S. Const. amend. V.

But there is a far more plausible interpretation of the Cures Act and its implementing regulations that does not require wading into this constitutional morass: namely, in seeking to increase interoperability and access, Congress did not demand that EHI custodians abandon their rights in their proprietary systems or intellectual property. Instead, Congress recognized that the definition of "information blocking" would not include "reasonable and necessary" activities, including protecting

EHI repositories from the risk of malicious attack, inadvertent damage or data corruption, or slowed performance occasioned by third-party applications using nonstandard access methods, and allowing the custodians of those repositories to charge reasonable fees for accessing them.

Because the district court's reading raises significant constitutional problems and a more plausible reading of the Act and its implementing regulations avoids those problems, this Court should reject the district court's interpretation. *See Hansen*, 599 U.S. at 781.

* * * *

RTMS did not establish a likelihood of success on its claim that PointClickCare violated federal law, so it cannot establish a likelihood of success on its state-law claims.

II. The State-Law Claims Fail For Independent Reasons.

Along with its misinterpretation of the Cures Act, the district court's state-law analysis was also plagued by other reversible errors.

No Private Right of Action. The Cures Act's information-blocking definitions make sense only within Congress's enforcement regime—which does not provide a private right of action. *See* R.21-1 at

1, 8. Where there is a claim of information blocking, the Cures Act delegates authority to the HHS OIG to investigate that claim. 42 U.S.C. § 300jj-52(b)(1). Only "following an investigation conducted under this subsection" can the OIG subject an entity engaged in information blocking to "a civil monetary penalty determined by the Secretary." *Id.*§ 300jj-52(b)(2). The OIG may also "refer such instances of information blocking to the Office for Civil Rights of" HHS for resolution. *Id.* § 300jj-52(b)(3). And once OIG determines an entity committed information blocking, the entity is subject to additional federal disincentives. *Id.* § 300jj-52(b)(2)(B). Congress created this enforcement regime for a reason—HHS has expertise in data privacy and security and can balance the potentially competing interests between parties in information-access disputes.

The district court concluded that the violation of the Cures Act could constitute unfair competition even though "the statute does not afford the plaintiff a private cause of action." JA1006-1007 (citing Restatement (Third) of Unfair Competition § 1, cmt. g (1995)). But the court skipped the analysis that the Restatement requires. A private cause of action sounding in tort based on a statutory violation is available

only where it "is not inconsistent with … legislative intent." Restatement (Third) of Unfair Competition § 1, cmt. a. And under Maryland law, a plaintiff cannot "predicate a State law claim for unfair competition on a purported violation of" a federal regulation when that regulation lacks a private right of action. *Waypoint Mgmt. Consulting, LLC v. Krone*, 2022 WL 2528465, at *61 (D. Md. July 6, 2022). In *Waypoint*, the court held that "even assuming defendants' conduct amounts to a violation of [the securities regulation], this cannot, on its own, establish defendants' liability as a matter of Maryland law." *Id.*

Other courts have also rejected common-law unfair-competition claims predicated on statutes or regulations with no private right of action. *See, e.g.*, *Checker Cab Phila., Inc. v. Uber Techs., Inc.*, 689 F. App'x 707, 709 (3d Cir. 2017) ("Whatever the breadth of unfair competition in Pennsylvania, state law clearly does not contemplate that violation of licensing regulations constitutes 'unfair competition.'"); *O'Donnell v. Bank of Am., Nat'l Ass'n*, 504 F. App'x 566, 568 (9th Cir. 2013) (affirming dismissal of an unfair-competition claim "premised on … violation of the Federal Trade Commission Act" because "[t]he federal statute doesn't create a private right of action, ... and plaintiffs

can't use California law to engineer one"); *Phila. Taxi Ass'n v. Uber Techs., Inc.*, 218 F. Supp. 3d 389, 394-95 (E.D. Pa. 2016) (plaintiffs' "claim necessarily fails … as it is premised on violations of state and local regulations [that] do not create a private right of action"); *Reeves v. PharmaJet, Inc.*, 846 F. Supp. 2d 791, 797 (N.D. Ohio 2012) (plaintiffs "may not use other federal statutes or state unfair competition laws as a vehicle to bring a private cause of action that is based on violations of the FDCA" (cleaned up)). Courts have rejected tortious-interference claims for the same reason. *See, e.g.*, *Vilcek v. Uber USA, LLC*, 902 F.3d 815, 820-21 (8th Cir. 2018) (affirming the dismissal of a tortious-interference claim based on the violation of statutes because they did not provide a private right of action).

A private right of action is inconsistent with the Cures Act. Under the statute, only HHS can define what constitutes information blocking, and only the OIG enforces that decision. *See* Restatement (Second) of Torts § 874A(h) (1979) (cited by Restatement (Third) of Unfair Competition § 1, cmt. a); *see also Johnson v. Kraft Gen. Foods, Inc.*, 885 S.W.2d 334, 336-37 (Mo. 1994) (en banc) (declining to find a private right of action where the legislature authorized a particular agency to enforce

the statute). Tort actions are blunt instruments that will interfere with the enforcement scheme Congress created. Restatement (Second) of Torts § 874A(h). And the proliferation of such lawsuits will burden courts and require them to wade into complex technological security issues in a world quickly evolving to respond to new dangers, new malicious actors, and new technology. *See id.*

Moreover, because the district court's interpretations of state law interfere with Congress's EHI-sharing-and-protection scheme, they are preempted in any event. *See Guthrie v. PHH Mortg. Corp.*, 79 F.4th 328, 336 (4th Cir. 2023) ("Federal law preempts—or bars—claims under state law that either interfere with or are contrary to federal law."). It makes no difference that RTMS seeks to lever open PointClickCare's repository using a state *tort* claim instead of a state *statute*—federal law trumps them both. *See, e.g.*, *Edwards v. CSX Transp. Inc.*, 983 F.3d 112, 120 (4th Cir. 2020) (holding tort claims preempted by federal statute).

The Cures Act is not designed to serve as the predicate for a tort claim. On that basis alone, this Court should reverse.

Tortious interference. Neither RTMS nor the district court seemed to know whether RTMS's claim is for tortious interference *with*

contract or tortious interference *with prospective business relationships*. RTMS bears the burden to identify on which version of the tort it was "likely to succeed." Because the district court cited a case assessing a tortious-interference-with-contract claim, PointClickCare presumes that is the claim the court assessed.

RTMS's tortious-interference claim fails because PointClickCare's generally-applicable bot-blocking was not directed at damaging RTMS. To establish a claim for tortious interference, RTMS must prove both that PointClickCare's interference was wrongful *and* done "with the unlawful purpose to cause … damage" to RTMS. *Painter's Mill Grille, LLC v. Brown*, 716 F.3d 342, 353-54 (4th Cir. 2013).

Here, RTMS cannot show that PointClickCare acted with tortious intent by enforcing standard contractual provisions. PointClickCare implemented CAPTCHAs to safeguard the security and integrity of its system against any high-volume bot. *See generally* JA234-256. The evidence shows that PointClickCare has applied CAPTCHAs against *all* suspected high-volume bot users for years. JA245 ¶ 29; JA202-203 §§ 2.1-2.2. The overwhelming majority of bot users PointClickCare has watch-listed are not associated with RTMS. JA245 ¶ 29; JA202-203

§§ 2.1-2.2; JA1532-1547. Indeed, before this litigation, PointClickCare *did not know* which user IDs RTMS used, so it *could not* have targeted RTMS. JA710 (Tr. 34:8-11).

The district court simply ignored this element of RTMS's claim, nowhere finding that PointClickCare's conduct was "directed at an existing prospective economic relationship" of RTMS's. *Interphase Garment Sols., LLC v. Fox Television Stations, Inc.*, 566 F. Supp. 2d 460, 465 (D. Md. 2008) (proving tortious interference requires a plaintiff to "show that the defendant's conduct was directed at an existing or prospective economic relationship and not a mere incidental effect of the allegedly wrongful conduct") (cleaned up). Instead, the district court concluded that RTMS could show tortious interference merely by showing that PointClickCare knew that implementing its no-bot contract provisions *could* interfere with RTMS's business. JA1016.

That is not the law. "[A]cting to pursue one's own business interests at the expense of others is not, in itself, tortious.'" *Alexander & Alexander Inc. v. B. Dixon Evander & Assocs., Inc.*, 650 A.2d 260, 269 (Md. 1994). It is undisputed that bot use causes performance problems. JA1003. It is undisputed that PointClickCare bans bot use by all its customers and

their agents. JA995. And it is undisputed that PointClickCare deployed its CAPTCHAs against all suspected bots, the vast majority of which were not using RTMS user IDs. JA245 ¶ 29; JA202-203 §§ 2.1-2.2; JA712 (Tr.36:8-10) ("Q. How many of the [600] user IDs on the watch list were on that Real Time list? A. 119.").

In addition, even if the Court had focused on tortious interference with RTMS's *contracts* rather than tortious interference with RTMS's business relations, there is no evidence that PointClickCare knew what RTMS's contracts require or prohibit. In fact, RTMS's contracts do not require bot access. JA440 (Tr.65:13-18). RTMS can perform its contracts for its customers through humans accessing the PointClickCare system, just as those customers themselves do. *See* JA509-510 (Tr.134:22–135:1) (conceding that RTMS could hire employees to access the necessary EHI).

The evidence shows that PointClickCare treated RTMS just as it treats every other comparable business. PointClickCare has never prevented RTMS from using its clients' login credentials to access information when those credentials are used only by humans. JA254 ¶ 51. Nor has PointClickCare prohibited RTMS from accessing the platform through a Marketplace API or the USCDI Connector program

used by numerous other vendors, including RTMS's competitors (which under the district court's logic would be PointClickCare's competitors too). JA289-291 ¶¶ 9, 12, 14; JA1295. Nothing in the record shows that PointClickCare's use of CAPTCHAs was "directed at" RTMS's economic relationships. *See Interphase*, 566 F. Supp. 2d at 465 (quotation marks omitted).

Unfair Competition. The "general principle" underlying Maryland unfair-competition law is that "all dealings must be done on the basis of common honesty and fairness, without taint of fraud or deception." *Balt. Bedding*, 34 A.2d at 342; *Paccar Inc. v. Elliot Wilson Capitol Trucks LLC*, 905 F. Supp. 2d 675, 692 (D. Md. 2012). Even if RTMS could prove that PointClickCare's implementation of its standard contract provisions somehow violated the Cures Act (which it cannot), RTMS cannot show that PointClickCare engaged in any sort of fraud or deception. That is fatal to its unfair-competition claim. PointClickCare enforced clear contract provisions that it has had with its customers for years. And PointClickCare offered to supply RTMS with EHI through a standard format or through Marketplace. PointClickCare has not tried

to trick or deceive RTMS or any other entity; it is simply trying to prevent third-party bots from running on its system.

III. The District Court Erred In Analyzing The Remaining Preliminary Injunction Factors.

The court's analyses of irreparable harm, the balance of equities, and the public interest were also infected by legal error.

Irreparable Harm/Balance of the Equities. To start, the court erred in finding irreparable harm. "[E]xtra inconvenience" does not "rise[] to the level of irreparable harm." *Molloy v. Metro. Transp. Auth.*, 94 F.3d 808, 813 (2d Cir. 1996) (vacating injunction where there were "less convenient" "alternatives"); *see also HCI Techs., Inc. v. Avaya, Inc.*, 241 F. App'x 115, 121, 124 (4th Cir. 2007) (per curiam) (affirming conclusion that plaintiff did not show irreparable harm given available alternatives).

The district court concluded that PointClickCare's "deployment of unsolvable CAPTCHAs visits on Real Time a 100% business interruption with any given nursing facility." JA1017. To reach that conclusion, the district court turned a blind eye to numerous alternatives available to RTMS. RTMS could still access all the EHI for a nursing facility through its human employees—and it could, moreover, have hired enough human

employees to satisfy its data demands. JA509-510 (Tr.134:22-135:1). RTMS could have agreed to the Marketplace terms PointClickCare proposed, allowing it to continue serving its customers in a fashion that did not burden PointClickCare's systems. Or RTMS could have opted to receive USCDI data, which would prevent it from suffering a "100% business interruption." Any interruption would be measurable and thus redressable by ordinary monetary damages—if any were due, and none are. The failure to consider these alternatives at all, much less account for them, is legal error. *See Hope v. Warden York Cnty. Prison*, 972 F.3d 310, 333 (3d Cir. 2020) (vacating TROs in part because "the Court failed to explore alternatives to avoid any irreparable harm").

The court further erred as a matter of law in accepting RTMS's "mere say-so" claim of business interruptions. *Braintree Labs., Inc. v. Citigroup Glob. Mkts. Inc.*, 622 F.3d 36, 42 (1st Cir. 2010) (party's "mere say-so is insufficient" to establish irreparable harm). RTMS's conclusory statements are not enough. *See, e.g.*, *Hamrick v. Quinlin*, 956 F.2d 1162, 1992 WL 38159, at *1 (4th Cir. 1992) (per curiam) (affirming denial of an injunction because plaintiff's "'conclusory' statements were insufficient to prove that he would suffer irreparable harm absent injunctive relief");

Noya v. Frontier Adjusters, Inc., 2013 WL 2490360, at *6 (D. Md. June 7, 2013) (denying preliminary relief in part because movant could not "clearly" show claimed harm was "imminent"). Where a movant claims that its business will collapse or people will be physically harmed, the movant must provide detailed evidence. *See, e.g.*, *SAS Inst., Inc. v. World Programming Ltd.*, 874 F.3d 370, 386 (4th Cir. 2017) (affirming denial of permanent injunctive relief where claims of "lost business relationships, market share, and goodwill were largely unsupported by the evidence"); *Diskriter, Inc. v. Alecto Healthcare Servs. Ohio Valley LLC*, 2018 WL 555720, at *5 (W.D. Va. Jan. 25, 2018) (denying preliminary injunction where movant provided no "financial documentation" to support claim of imminent business harm); *Boyer v. Taylor*, 2012 WL 1132786, at *3 (D. Del. Mar. 30, 2012) ("The plaintiffs allege in a conclusory manner that the failure to issue injunctive relief could result in death or severe illness. The plaintiffs provide argument, but no evidence …. The plaintiffs fail to meet the requisites for injunctive relief."). RTMS provided nothing to back up its unvarnished *ipse dixit*.

The district court's decision also severely underestimated the harm to PointClickCare and the public. First, the court-ordered rollback of

PointClickCare's security system for RTMS's bots threatens the stability of PointClickCare's system. Unpredictable, high-volume bot activity causes system crashes and slowdowns, which put patient lives at risk because doctors and nurses cannot timely access the medical records necessary to administer medication and make life-saving decisions. PointClickCare's system handles 1.2 million such transactions every day. JA808 (Tr.132:9-13).

Moreover, not being able to block high-volume bots that are extracting data from PointClickCare's system creates a massive security gap. Much was made of RTMS's security certifications at the hearing, *e.g.*, JA523 (Tr.148:10-17), but those certifications mean only that EHI exfiltrated from PointClickCare by RTMS's bots is less likely to be exfiltrated from RTMS by someone else's bot or other unauthorized means.

Ironically, while the district court lauded RTMS's purported security certification, the court's order precludes PointClickCare from securing its own systems. There is no assurance that the bots using RTMS user IDs will always be RTMS's bots, because malicious actors can obtain user IDs and spoof IP addresses. JA488-489 (Tr.113:24-114:6).

And the injunction bars PointClickCare from proactively blocking such malicious activity and preventing any resulting data breach—which risks devastating injury to its customers and their patients, yielding devastating damages to PointClickCare. JA979 (Tr.303:11-15). The district court's imposition of a $50,000 bond, JA1018, shows that it vastly underestimated—or failed to consider—the magnitude of liability from such a breach.

Public Interest. The court also misapprehended the impact of its injunction on the public interest. Overturning the preliminary injunction will preserve Congress's harmonization of competing objectives reflected in the Cures Act, HIPAA, the HITECH Act, and the CFAA. Absent reversal, all of PointClickCare's customers' EHI—1.6 million patients' worth—is at risk. JA235, JA250-251, JA255 ¶¶ 5, 41-43, 56; JA293 ¶¶ 20-21. The public has a strong interest in ensuring the integrity of systems protecting EHI. *See Hum. Touch DC, Inc. v. Merriweather*, 2015 WL 12564166, at *5 (D.D.C. May 26, 2015) (citing the public's "powerful interest" in the integrity of its "health information").

CONCLUSION

For the foregoing reasons, PointClickCare respectfully requests that the Court reverse and vacate the injunction.

Respectfully submitted,

/s/Jeremy M. Bylund

Rod J. Rosenstein
Jeremy M. Bylund
Counsel of Record
Amy R. Upshaw
Joshua N. Mitchell
KING & SPALDING LLP
1700 Pennsylvania Avenue NW
Washington, DC 20006
(202) 737-0500
jbylund@kslaw.com

William C. Jackson
GOODWIN PROCTER LLP
1900 N Street NW
Washington, DC 20036

Nicole Bronnimann
KING & SPALDING LLP
1100 Louisiana Street
Suite 4100
Houston, TX 77002

Counsel for PointClickCare Technologies Inc.

September 16, 2024

CERTIFICATE OF COMPLIANCE

This motion complies with the type-volume limitation of Fed. R. App. P. 32(a)(7), because it contains 12,961 words, excluding the parts of the motion exempted by Fed. R. App. P. 27(a)(2)(B) and 32(f).

This motion complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6), because it has been prepared in a proportionally spaced typeface using Microsoft Word 365 in Century Schoolbook 14-point font.

Date: September 16, 2024

/s/ Jeremy M. Bylund
Jeremy M. Bylund

Counsel for PointClickCare Technologies Inc.